

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-183866

(43)Date of publication of application : 30.06.2000

(51)Int.Cl. H04L 9/08  
G09C 1/00  
H04L 9/14

(21)Application number : 10-351857

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 10.12.1998

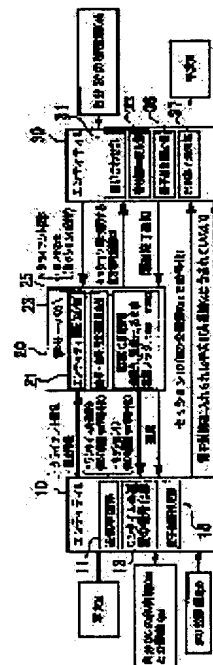
(72)Inventor : HATAJIMA TAKASHI

## (54) METHOD AND SYSTEM FOR CIPHER COMMUNICATION, AND RECORDING MEDIUM STORED WITH CIPHER COMMUNICATION PROGRAM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To confirm if a communication sentence is transferred to the other party being safe and legal by generating either a common key or a session ID and transmitting the communication text with either of them utilized for an electronic envelope.

**SOLUTION:** A transmission application part 11 of an entity A10 transmits destination information to a key server C20 and requests client authentication. A decoding part 13 of a one-time common key decodes a one-time common key Kc transmitted from the server C20 and takes out the key Kc. And, an electronic envelope preparing part 15 enters a communication text M of plaintext to be transmitted to a receiving client B by a transmitting client A into an electronic envelope E and directly transmits it to an entity B30 without going through the server C20. Further, a key use state managing part 25 issues a session ID which is generated by a random number generator including a session ID proper to this transaction and is enciphered to a public key with the public key Kpc of the server C20 and a public key Kpb of the transmission destination entity B30 in each transmission destination.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2000-183866  
(P2000-183866A)

(43)公開日 平成12年6月30日 (2000.6.30)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E
			6 6 0 G
H 0 4 L 9/14		H 0 4 L 9/00	6 0 1 E
			6 4 1
審査請求 未請求 請求項の数12 O L (全 8 頁)			

(21)出願番号 特願平10-351857

(22)出願日 平成10年12月10日 (1998.12.10)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 畑島 隆

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74)代理人 100083806

弁理士 三好 秀和 (外1名)

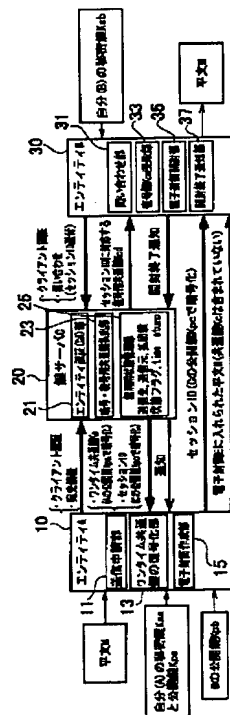
Fターム(参考) 5J104 AA01 AA16 EA02 EA19 EA23  
NA02 NA03 NA27 PA07

(54)【発明の名称】 暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体

(57)【要約】

【課題】 本発明は、より安全でかつ正当な相手に届けられたか送達確認が可能な暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体を提供することを目的としたものである。

【解決手段】 電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであって、少なくとも共通鍵とIDのいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／およびIDを電子封筒に利用して伝達文を送信することを特徴とする。



## 【特許請求の範囲】

【請求項 1】 伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、送信元から送信先に送信する際に、少なくとも共通鍵とセッション ID のいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信することを特徴とする暗号通信方法。

【請求項 2】 前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを特徴とする請求項 1 記載の暗号通信方法。

【請求項 3】 前記共通鍵とセッション ID が鍵サーバで生成されるとき、送信先は、送信先から送られてきたセッション ID による鍵サーバへの問い合わせの結果、鍵サーバから送られてきた送信先の公開鍵により公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得るとき、鍵サーバへ開封終了通知を行い、この開封終了通知を受けた鍵サーバは送信元へ着信完了通知を送ることを特徴とする請求項 1 記載の暗号通信方法。

【請求項 4】 伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、送信元から送信先に電子封筒を送信する際に、セッション ID を都度生成し、このセッション ID を同送することにより暗号通信のセッション管理を行うことを特徴とする暗号通信方法。

【請求項 5】 前記セッション管理は、鍵サーバの公開鍵で暗号化されたセッション ID を暗号通信のトランザクションの際に受け渡すことで行うことを特徴とする請求項 4 記載の暗号通信方法。

【請求項 6】 電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであって、少なくとも共通鍵とセッション ID のいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／および ID を電子封筒に利用して伝達文を送信することを特徴とする暗号通信システム。

【請求項 7】 前記共通鍵が鍵サーバで生成されるとき、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを特徴とする請求項 6 記載の暗号通信システム。

【請求項 8】 前記共通鍵が鍵サーバで生成されるとき、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得ることを特徴とする請求項 7 記載の暗号通信システム。

【請求項 9】 前記共通鍵とセッション ID が鍵サーバで生成されるとき、前記送信元は鍵サーバが自身の秘密鍵により公開鍵暗号化した共通鍵払い出しに対するセッ

ション ID を送信先へ伝達文とともに送り、送信先は送信元から送付されたセッション ID を鍵サーバへ送り、鍵サーバは自身の秘密鍵で復号化して得られる平文のセッション ID に対応する共通鍵を送信先の公開鍵で暗号化して送信先へ送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封して平文の伝達文を得、さらに送信先は復号完了の後に鍵サーバに前記セッション ID を送り返し、鍵サーバは送信元へ着信・復号完了通知を送ることを特徴とする請求項 8 記載の暗号通信システム。

【請求項 10】 伝達文を電子封筒に入れて送信元から送信先に送信する際に、少なくとも共通鍵とセッション ID のいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信する暗号通信プログラムを記録した記録媒体。

【請求項 11】 伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵を生成すると共に、送信元はこの共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成して伝達文を送信する暗号通信プログラムを記録した記録媒体。

【請求項 12】 伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵とセッション ID が鍵サーバで生成され、この鍵サーバは送信元へ着信完了通知を送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得る暗号通信プログラムを記録した記録媒体。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、電子封筒を用いた暗号通信の際の安全性を高めると共に、送信先への送達完了を確認し得るようにした暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体に関するものである。

【0002】

【従来の技術】 従来、電子封筒を用いた暗号通信としては、S/MIME (Secure/Multipurpose Internet Mail Extensions) が安全なメッセージ送信方式の一つとして知られている。この S/MIME は、公開鍵暗号、共通鍵暗号、一方向暗号を使用して、文書の暗号化と改竄、成りすましを防止している。具体的には、図 3 および図 4 に示すように、S/MIME では、共通鍵 Kc は送信先の公開鍵 Kpb で暗号化され、電子封筒 E に内包されて、平文の伝達文 M と共に送信先へ送信される。このため、電子封筒 E が解読されたら、共通鍵 Kc が判るため、確実に解読されてしまうことになる。

【0003】 また、通信路を暗号化するものとしては、SSL (Secure Sockets Layer) が知られるが、これ

は、例えばクライアントとサーバとの間で、クライアント認証およびデータについて認証が行われる場合のような、一対一通信にのみ適用が可能である。

【0004】

【発明が解決しようとする課題】 上述したような暗号通信に対して、安全性に不安がある、送達確認ができない、正当な相手に届けられたかが分からない、そのため厳密な商取引には向かない等の問題点が指摘されていた。

【0005】 本発明は、上記課題に鑑みてなされたもので、より安全でかつ正当な相手に届けられたか送達確認が可能な暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体を提供することを目的としたものである。

【0006】

【課題を解決するための手段】 前述した目的を達成するために、本発明のうちで請求項 1 記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、送信元から送信先に送信する際に、少なくとも共通鍵とセッション ID のいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信することを要旨とする。

【0007】 請求項 1 記載の本発明にあつては、少なくとも共通鍵とセッション ID のいずれか一つが電子封筒に利用されることから、より安全でおよび／または送達確認が可能となる。

【0008】 請求項 2 記載の発明は、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを要旨とする。

【0009】 請求項 2 記載の本発明にあつては、共通鍵が送信先の公開鍵で暗号化されることからより安全性を高めることができる。

【0010】 請求項 3 記載の発明は、前記共通鍵とセッション ID が鍵サーバで生成されるとき、送信先は、送信先から送られてきたセッション ID による鍵サーバへの問い合わせの結果、鍵サーバから送られてきた送信先の公開鍵により公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得るとき、鍵サーバへ開封終了通知を行い、この開封終了通知を受けた鍵サーバは送信元へ着信完了通知を送ることを要旨とする。

【0011】 請求項 3 記載の本発明にあつては、セッション ID がハンドリングされることから、伝達文の送信先への着信を確実に確認することができる。

【0012】 請求項 4 記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であつて、送信元から送信先に電子封筒を送信する際に、セッション ID を都度生成し、このセッション ID を同送することにより暗号通信のセッション管理を行う

ことを要旨とする。

【0013】 請求項 5 記載の発明は、前記セッション管理は、鍵サーバの公開鍵で暗号化されたセッション ID を暗号通信のトランザクションの際に受け渡すことで行うことを要旨とする。

【0014】 請求項 6 記載の発明は、電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであつて、少なくとも共通鍵と ID のいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／および ID を電子封筒に利用して伝達文を送信することを要旨とする。

【0015】 請求項 7 記載の発明は、前記共通鍵が鍵サーバで生成されるとき、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを要旨とする。

【0016】 請求項 8 記載の発明は、前記共通鍵が鍵サーバで生成されるとき、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得ることを要旨とする。

【0017】 請求項 9 記載の発明は、前記共通鍵とセッション ID が鍵サーバで生成されるとき、前記送信元は鍵サーバが自身の秘密鍵により公開鍵暗号化した共通鍵払い出しに対するセッション ID を送信先へ伝達文とともに送り、送信先は送信元から送付されたセッション ID を鍵サーバへ送り、鍵サーバは自身の秘密鍵で復号化して得られる平文のセッション ID に対応する共通鍵を送信先の公開鍵で暗号化して送信先へ送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封して平文の伝達文を得、さらに送信先は復号完了の後に鍵サーバに前記セッション ID をを送り返し、鍵サーバは送信元へ着信・復号完了通知を送ることを要旨とする。

【0018】 請求項 10 記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、少なくとも共通鍵とセッション ID のいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信する暗号通信プログラムを記録した記録媒体であることを要旨とする。

【0019】 請求項 11 記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵を生成すると共に、送信元はこの共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成して伝達文を送信する暗号通信プログラムを記録した記録媒体であることを要旨とする。

【0020】 請求項 12 記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵と

セッションIDが鍵サーバで生成され、この鍵サーバは送信元へ着信完了通知を送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得る暗号通信プログラムを記録した記録媒体であることを要旨とする。

【0021】請求項10、11、12記載の本発明にあつては、暗号通信プログラムを記録媒体として記録しているため、該記録媒体を利用して、その暗号通信プログラムの流通性を高めることができる。

【0022】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0023】図1は本発明の一実施の形態に係る暗号通信システムの構成を示すブロック図である。

【0024】本実施形態の暗号通信システムは、送信クライアントAの送信端末として機能するエンティティA10、セッション管理機能を持つ鍵サーバC20及び受信クライアントAの受信端末として機能するエンティティB30によって構成される。また鍵サーバC20はエンティティA10とエンティティB30との間に設けられる。なお、後述するように本実施形態では、セッションIDは、鍵サーバC20が鍵サーバ自身の公開鍵Kpで公開鍵暗号化したものであり、送信元、送信先ではともに復号することはないものである。また、同様に共通鍵Kcは、鍵サーバC20が送付相手の公開鍵Kpで公開鍵暗号化したものであり、送り付けられた人は自身の秘密鍵Ksを用いて復号することができる。

【0025】また、エンティティA10は、送信申請部11、ワнтаイム共通鍵の復号化部13及び電子封筒作成部15を有し、鍵サーバC20は、エンティティ認証(CA)部21、鍵利用状態管理部23を有し、さらにエンティティB30は問い合わせ部31、復号鍵受取部33、電子封筒開封部35及び開封終了通知部37を有している。

【0026】エンティティA10の送信申請部11は送信クライアントAから伝達文の送信の依頼があつたときに鍵サーバC20に対し宛先情報を送信すると共にクライアント認証を依頼する機能を有し、ワнтаイム共通鍵の復号化部13は鍵サーバC20から送信されたワнтаイム共通鍵Kc(自身、つまり送信クライアントAの公開鍵Kpaで暗号化されている)を復号し、ワнтаイム共通鍵Kcを取り出す機能を有し、電子封筒作成部15は送信クライアントAが受信クライアントBに送信しようとしている平文の伝達文M(以下、単に平文M)を電子封筒Eに入れ、鍵サーバC20を介すること無く直接エンティティB30に対し送信する機能を有する。

【0027】また、鍵サーバC20のエンティティ認証(CA)部21は、各エンティティの認証、つまり該鍵サーバC20が予め発行したクライアント証明書につい

て認証する機能を有し、暗号・復号用共通鍵抽出部23は送信側に対しては暗号用の共通鍵Kcを、受信側に対しては復号用の共通鍵Kcを生成し払い出す機能を有し、鍵利用状態管理部25は本トランザクションに固有なセッションIDを内蔵する乱数発生器により発生し、鍵サーバC20の公開鍵Kpcで公開鍵暗号化したセッションIDと、送信先エンティティB30の公開鍵Kpbとを送信先ごとに発行する機能を有する。

【0028】さらに、エンティティB30の問い合わせ部31は先にエンティティA10から送信されたセッションID(鍵サーバC20の公開鍵Kpcで暗号化されている)を鍵サーバC20に送付し問い合わせを行う機能を有し、復号鍵受取部33は鍵サーバC20に送付したセッションIDに対応する復号用共通鍵Kcd(エンティティB30の公開鍵Kpbで暗号化されている)を鍵サーバC20から受け取る機能と、暗号化されている復号用の共通鍵Kcbを自身の秘密鍵で復号する機能を有し、電子封筒開封部35はエンティティA10から送信された電子封筒Eを受信すると共に開封する機能を有し、開封終了通知部37は電子封筒開封部35における開封処理を受けて鍵サーバC20に開封終了通知を送信する機能を有する。

【0029】次に図2を参照して、本実施形態をより具体的に処理手順に従って説明する。本実施形態では各エンティティ(送信元エンティティA10、送信先エンティティB30)は、予め、それぞれ鍵サーバC20(図2では実際に鍵サーバとして機能するエンティティCを鍵ブローカとして記載している)から電子証明書の発行を受けている。

【0030】まず、送信元エンティティA10は、ステップS1で鍵サーバC20に対し送信先エンティティB30を申告する。

【0031】鍵サーバC20は、ステップS2で送信元エンティティA10の認証を行い、該認証が正常に終了したときには、本トランザクションにのみ有効な共通鍵Kcを、エンティティA10の公開鍵Kpaで暗号化して送信元エンティティA10に送付する。また、このとき本トランザクションに固有なセッションIDを乱数発生器により発生し、鍵サーバC20の公開鍵Kpcで暗号化したセッションIDと、送信先エンティティB30の公開鍵Kpbを送信元エンティティA10に送信する。

【0032】なお、このとき鍵サーバC20では、送信元エンティティA10からの申告に伴い、送信元(ここではエンティティA10)、送信先(ここではエンティティB30)、要求時刻、発行した共通鍵KcおよびセッションIDを鍵利用状態管理部25に設けられる管理テーブルに記録しておく。また、この管理テーブルへは送信先の数だけレコードを追加するものとする。

【0033】また、鍵サーバC20から送信元エンティ

## 7

ティ A10 へ送られる共通鍵 Kc は、送信元エンティティ A10 の公開鍵 Kpa を用いて公開鍵暗号方式で暗号化されている。また鍵サーバ C20 からのセッション ID も、前述したようにすでに鍵サーバ C20 の公開鍵 Kpc で公開鍵暗号化されている。

【0034】次に、ステップ S3 において、送信元エンティティ A10 は、鍵サーバ C20 から得た A の公開鍵 Kpa で暗号化した共通鍵 Kc を、自身の秘密鍵 Ksa を使って復号し、共通鍵 Kc とセッション ID を得る。

【0035】送信元エンティティ A10 は、ステップ S4 で、以下に後述するいずれかの手段により選ばれた（データ A、B）、もしくは、（データ C、D）の組と共通鍵 Kc とをまとめて送信先エンティティ B30 の公開鍵 Kpb で暗号化し、電子封筒 E を作成する。

【0036】なお、このとき送信元エンティティ A10 が、以下のいずれかの手段により選ばれた（データ A1、A2）、もしくは（データ B1、B2）の組をまとめて送信先エンティティ B30 の公開鍵 Kpb で暗号化し、電子封筒 E を作成するようにしても良い。つまり、この実施形態の場合には、共通鍵 Kc を電子封筒 E に含めていない。

【0037】（データ A1、A2）

データ A1；平文 M に対してハッシュ関数を用いて電子署名する。電子署名を送信元エンティティ A10 の秘密鍵 Ksa で公開鍵暗号化する。

データ A2；平文 M を共通鍵 Kc で共通鍵暗号化する。

【0038】（データ B1、B2）

データ B1；平文 M を共通鍵 Kc で共通鍵暗号化する。

データ B2；データ B1 をハッシュ関数を用いて電子署名する。電子署名を送信元エンティティ A10 の秘密鍵 Ksa で公開鍵暗号化する。

【0039】次に、ステップ S5 で、送信元エンティティ A10 は、セッション ID と電子封筒 E を送信先エンティティ B30 へ送信する。

【0040】送信先エンティティ B30 は、ステップ S6 で、暗号文が到着したことを鍵サーバ C20 に通知する。この通知は、前述のセッション ID（鍵サーバ C20 の公開鍵 Kpc で暗号化したもの）を鍵サーバ C20 に送信することによって行う。

【0041】鍵サーバ C20 は、ステップ S7 で、受信したセッション ID を、自身の秘密鍵 Ks で復号化し、平文となったセッション ID が記載されているレコードを管理テーブルから探す。このレコードに記載されている共通鍵 Kc を送信先エンティティ B30 の公開鍵 Kpb で公開鍵暗号化して送信先エンティティ B30 へ送付する。

【0042】送信先エンティティ B30 は、ステップ S8 で鍵サーバ C20 から送られた公開鍵暗号化された共通鍵 Kc を、自身の秘密鍵 Ksb を用いて復号する。さらに復号された共通鍵 Kc と送信元エンティティ A10

## 8

の公開鍵 Kpa を用いて、電子封筒 E を開封し、平文 M を得る（ステップ S9）。これにより送信先エンティティ B30 は、ステップ S10 で、鍵サーバ C20 に対して復号完了を通知する（セッション ID を送信）。

【0043】一方、鍵サーバ C20 は、この復号完了通知を受けて、ステップ S11 でレコードにある送信元エンティティ A10 へ着信完了通知を送る。これにより送信元エンティティ A10 は、伝達文の送信先エンティティ B30 への送達完了を確認する。なお、このときの通知手段はメール、専用プロトコルなど任意である。この着信完了通知の送信と同時に、鍵サーバ C20 は管理テーブルからレコードを削除する。

【0044】次に、他の実施形態について説明する。

【0045】ステップ S1 乃至 7、10 までは、前述した実施形態と同様なので説明を省略する。

【0046】鍵サーバ C20 の管理テーブルでは共通鍵送信済みフラグを立て、新規セッション ID を公開鍵暗号化して送信先エンティティ B30 へ送る。

【0047】送信先エンティティ B30 は、鍵サーバ C20 から送られた公開鍵暗号化された共通鍵 Kc を、自身の秘密鍵 Ksb を用いて復号する。復号された共通鍵 Kc と送信元エンティティ A10 の公開鍵 Kpa を用いて、電子封筒 E を開封し、平文 M を得る。

【0048】さらに送信先エンティティ B30 は復号完了したら、鍵サーバ C20 に通信新規セッション ID を送り返す。これにより鍵サーバ C20 は送信元エンティティ A10 へ着信・復号完了通知を送る。このときの通信手段はメール、専用プロトコルなど任意である。

【0049】なお、上述してきたような暗号通信システムは暗号通信プログラムにより実現され、該プログラムは記録媒体に記録して提供される。

【0050】上述してきたように、上記各実施形態によれば、鍵サーバからの ID 払い出しにより、セッション管理を可能にし、また鍵サーバにしか解読できないセッション ID をハンドリングすることによって通信セッション全体について安全性を確保している。すなわち、セッション管理により、いわゆる配達証明を可能にしたものである。

【0051】また、電子封筒に共通鍵を内包しない場合、電子封筒だけが解読されても、共通鍵を手に入れないと、内容を平文に出来ない分だけ S/MIME よりも解読が難しくなる。つまり、本文を高速な共通鍵暗号で暗号化する S/MIME の利点を生かしつつ安全性を高めたことになる。

【0052】さらに共通鍵は信頼できる鍵サーバから別途送られるため、攻撃される確率を低く出来、また共通鍵はトランザクション中の鍵受取者の公開鍵で暗号化されるため鍵受取者以外は復号することはできない。

【0053】耐成りすまし性は、電子証明書と、サーバにしか解読できないセッション ID による認証により確

10

20

30

40

50

保され、また耐改竄性は一方向暗号と電子証明書により安全性を保証している。

【0054】これを通常の郵便（郵政省管轄）になぞらえると、S/MIMEが（書留郵便＋内容証明）であるのに対し、本発明は（書留郵便＋内容証明＋配達証明）と表現される。

【0055】

【発明の効果】以上説明したように、本発明によれば、安全かつメッセージが到達されたことが確認可能な暗号通信システムを構築できる。

【図面の簡単な説明】

【図1】本発明に係る暗号データメッセージングシステムの一実施形態の全体構成図である。

【図2】本発明に係る暗号データメッセージングシステムの一実施形態における処理を示したデータフロー図である。

【図3】従来の暗号データメッセージングシステムの全

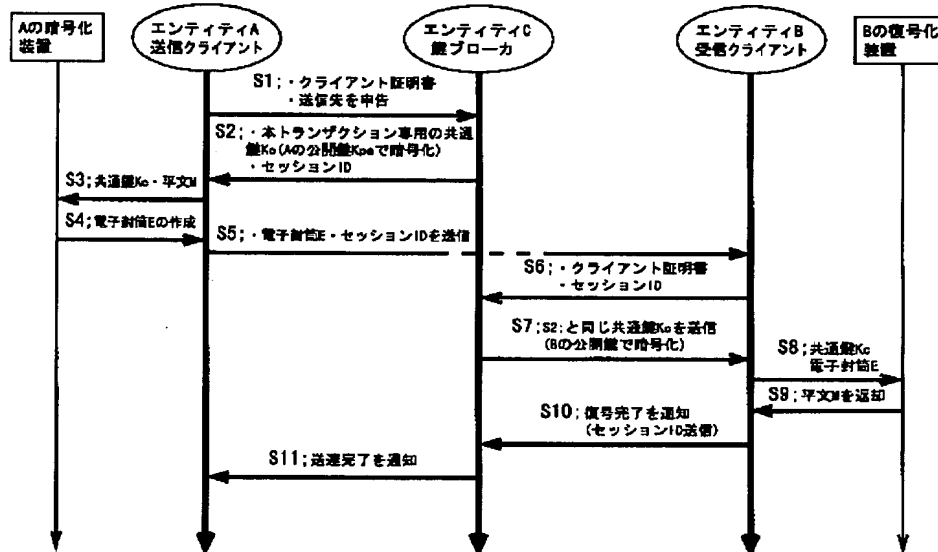
体構成を示すブロック図である。

【図4】従来の暗号データメッセージングシステムにおける処理を示したデータフロー図である。

【符号の説明】

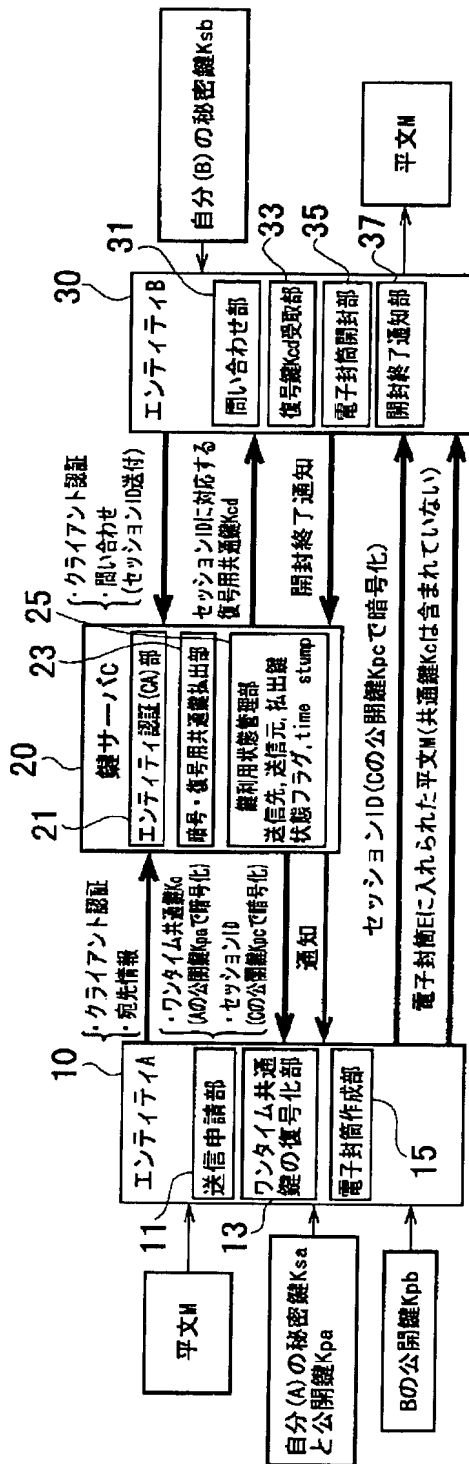
- 10 エンティティA
- 11 送信申請部
- 13 ワンタイム共通鍵の復号化部
- 15 電子封筒作成部
- 20 鍵サーバC
- 21 エンティティ認証（CA）部
- 23 鍵利用状態管理部
- 30 エンティティB
- 31 問い合わせ部
- 33 復号鍵受取部
- 35 電子封筒開封部
- 37 開封終了通知部

【図2】

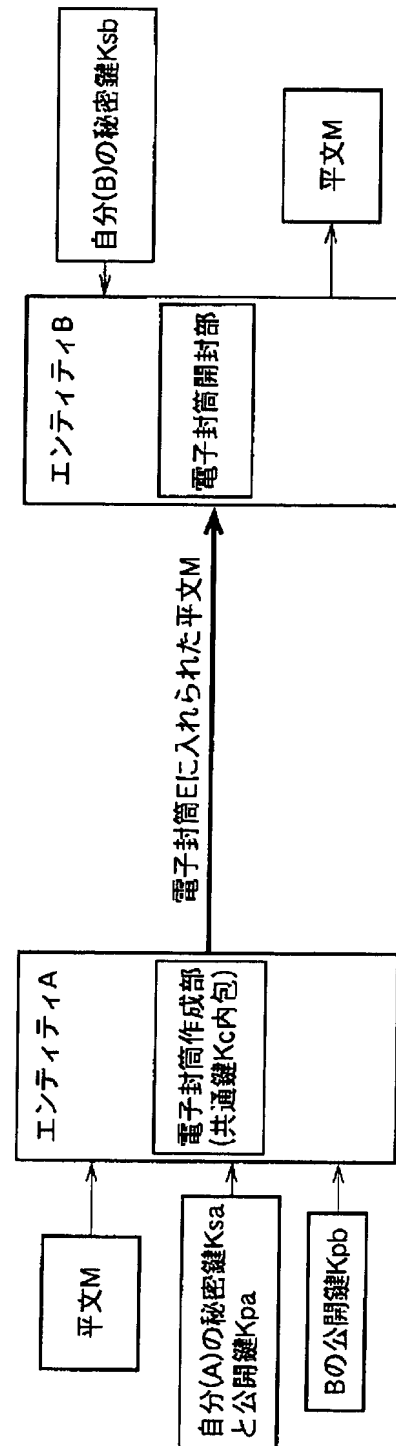




【図 1】



【図 3】



【図4】

